TESTIMONY OF SECRETARY MICHAEL CHERTOFF
U.S. DEPARTMENT OF HOMELAND SECURITY
BEFORE THE HOUSE COMMITTEE ON HOMELAND SECURITY
WASHINGTON, DC
WEDNESDAY, SEPTEMBER 5, 2007

INTRODUCTION

Chairman Thompson, Ranking Member King, and Members of the Committee: I appreciate the opportunity to testify today about the progress of our efforts to secure our homeland.

Before I continue, let me acknowledge the partnership between our Department and your Committee. Given the reality of rapidly evolving threats from terrorism and other dangers, our Department must respond creatively and comprehensively, but it cannot do it alone. It is only through your assistance in the legislative arena that we can continue to thwart the plans and strategies of our enemies in our post-September-11 world.

So let me take a moment to thank you for passing legislation that enhances the security of our Visa Waiver Program, protects people who report suspicious activity or behavior to the authorities, and allows for greater amounts of state Homeland Security grants to be distributed on a risk basis.

Next Tuesday will mark the sixth anniversary of the September 11 attacks. We will honor the memory of those who died that day, and remember in particular the heroic actions of those who gave their lives to save thousands of their fellow Americans.

On September 11, 2001, no one could have predicted the passage of six years without further attacks on our homeland.

By any measure, this is a remarkable achievement. It is the result of our comprehensive efforts to secure our safety, while maintaining our liberty and way of life, including our privacy. It is a tribute to the successes of our armed forces abroad and to our law enforcement efforts at home. It is a testament to our Customs and Border Protection (CBP) officers in keeping dangerous individuals and groups away from our country, to our Immigration and Customs Enforcement (ICE) personnel in removing those who got in, to our Coast Guard in protecting our ports and waterways, and to our Transportation Security Administration in the guarding of our airports and transit networks. It highlights the importance of improved information sharing across Federal agencies, and between Washington and our states and localities. It bears witness to the benefits of integration within our own Department. It is the result of the tireless efforts of our federal partners in homeland security, including the Department of Justice, the FBI and the Department of State. It underscores the importance of our relationship with Congress and particularly with this Committee.

Yet despite this accomplishment, our nation remains at risk. Clearly, our terrorist foes continue to plot against us and target our people and infrastructure. Over the past year, we helped disrupt a number of planned attacks, notably the plot last summer in London to hijack planes heading for America.

The good news is that these plots were thwarted. The more sobering news is that, these operational successes notwithstanding, the terrorist threat remains a potent one. This is further evidenced by the results contained in the July 2007 National Intelligence Estimate. According to the NIE report, America faces a continued threat from ideologically driven terrorist networks like Al Qaeda, which, while weaker than it was on 9/11, is growing again in strength. Moreover, we cannot discount the danger posed by homegrown terrorists, isolated individuals or groups that initiate their own plots after becoming radicalized.

The risks we confront continue to evolve and the potential targets across our nation are numerous indeed. If we tried to eliminate every risk, we would obviously fail. Moreover, we would become so heavy-handed with security, we would end up destroying exactly what we are trying to protect -- the normal, daily fabric of life across our nation.

So instead of trying to eliminate risk, our overarching strategy is to reduce and manage it. Risk management lets us identify what should concern us most in terms of threats, existing vulnerabilities, and potential consequences.

Our risk management philosophy drives all that we do. Accordingly, my testimony will refer to it frequently. I will focus on both our successes and our challenges. Mostly I will discuss threats that are man-made, but I will also note the challenges we face from nature. I will summarize what we have achieved over the past year, highlight what we aim to accomplish this year and for the future, and suggest how Congress can help us in these critical efforts to secure our nation.

A YEAR OF ACHIEVEMENTS

Last year, our Department formulated five specific goals to help us advance our mission of securing our homeland. These five goals include protecting America from dangerous individuals, protecting it from dangerous things, protecting our critical infrastructure, building a 21st century emergency response system and a culture of preparedness, and strengthening and unifying DHS operations and management.

I want to talk about this past year's achievements in the context of these five goals or priorities.

1. Protecting Against Dangerous People

The first of these priorities deals directly with individuals who seek to enter this country and do us harm.

Expanding our Perimeters/Intercepting Our Enemies Overseas

In response to this threat, our strategy begins by expanding our perimeters so that America's actual borders are not our first line of defense. Our aim is to intercept dangerous enemies abroad, before they reach our borders.

In order to do this, we need relevant information about travelers. To that end, this July, we reached a Passenger Name Record (PNR) agreement with the European Union in which the EU agreed to continue to provide our Department access to pertinent data from airliners on passengers taking transatlantic flights to and from the EU. We also collect this information on arrivals from other regions as well.

And just last month, responding to a recommendation of the 9/11 Commission, we enhanced our Advanced Passenger Information System (APIS) by publishing a final rule requiring international air and sea carriers to provide Customs and Border Protection (CBP) passenger manifest information prior to boarding, rather than when planes are already in flight, and cruise ships are underway.

Obviously, our PNR and APIS initiatives work in tandem. With both of these types of information, combined with the Automated Targeting System for Passengers, we have identified overseas passengers who have posed a real danger and prevented them from boarding planes destined for our country.

Since 9/11, PNR data have helped us significantly in combating potential threats.

In April 2006, at Boston's Logan Airport, CBP officers used PNR information to identify two passengers whose travel patterns exhibited high-risk indicators. During the secondary interview process, one subject stated that he was traveling here on business for a group that is suspected of having financial ties to Al Qaeda. The examination of his baggage revealed images of armed men, one of them labeled "Mujahadin." Both passengers were refused admission.

PNR and APIS will help us identify previously known overseas enemies before they can board a plane bound for our country and fingerprinting can also be useful in this process. Under our US-VISIT program, millions of non-citizens arriving here through ports of entry have their fingers scanned and then checked against the fingerprints we have from prior entries and their visa records in order to make sure that they are to whom the visa was granted and they're not felons or terrorists.

But what about detecting unknown enemies? Recently, we've taken a quantum leap forward and are poised to identify them for the first time. We are transitioning to 10-print collection, which we will run not only against databases of known dangerous individuals, but also against those we're collecting from battlefields, safe houses, and terrorist training camps around the world. This creates a powerful deterrent against any terrorist seeking to enter our country from any of these places.

Through our US-VISIT program, we're also continuing to run terrorist and criminal watch list checks, often across multiple databases maintained by separate agencies. Our goal is to ensure that US-VISIT is interoperable with the FBI fingerprint database. We're integrating our watch lists and recently we created the Traveler Redress Inquiry Program (DHS TRIP) to enable people who have been mistakenly placed on such lists to petition to be removed from them.

Secure Identification

Through PNR, APIS, and US-VISIT's 10-fingerprint initiative, we now have critical new or enhanced tools to help us identify lethal enemies -- including those previously unknown -- from among the numerous travelers who arrive from overseas.

But what do we do about enemies who deliberately masquerade as legitimate passengers? We address the critical need for secure travel documentation.

The 9/11 Commission spoke directly to this issue when it wrote these words, "[S]ources of identification are the last opportunity to ensure that people are who they say they are and to check whether they are terrorists."

The Commission put it well when it added, "For terrorists, travel documents are like weapons."

Indeed, when we investigated the 9/11 attacks, we discovered that 18 of the 19 perpetrators had been issued U.S. identification documents and that some of these documents had been obtained fraudulently.

Fraudulent documents are undeniably a growing problem. Since 2005, our CBP officers have intercepted more than 90,000 fraudulent documents and apprehended more than 60,000 people trying to enter our country with such documents.

Our CBP officers must wade through nearly 8,000 different kinds of travel documents we currently accept at our land border. There is no way these officers can quickly or effectively tell whether those documents are real or fraudulent. Obviously, this puts our nation at risk.

In response to this problem, in January of this year, we implemented our rule for the air travel portion of the Western Hemisphere Travel Initiative. WHTI requires people traveling to and from Canada, Mexico, the Caribbean, and Bermuda to present a passport or other approved identification document in order to enter or re-enter the United States. Secure documents are a national imperative that will prevent dangerous people from entering our country using fraudulent identification. WHTI will enhance our ability to assess threats and confirm identity at ports of entry, while continuing to facilitate lawful travel and commerce.

In June of this year, we published the proposed rule for WHTI's land and sea portion.

Border Security

Over the past year, we have continued our efforts to secure our homeland by taking strong steps to secure our land borders.

Since President Bush took office, our nation has added 5,000 new Border Patrol Agents, bringing the current total to more than 14,000. By the end of 2008, we will have more than 18,300, double the number we deployed before 2001.

Moreover, as part of ***Operation Jump Start***, thousands of National Guard members have been deployed to the southern border since June of last year. Up to 3,000 Guard members will continue this operation through July of next year.

We have also been putting more infrastructure in place. Today we have nearly 113 miles of fencing and 112 miles of vehicle barriers have been erected along the southern border. By the end of the current fiscal year, we expect to have 150 miles of fencing in place.

Besides adding more boots on the ground and more infrastructure, last year we abolished the practice of catch-and-release at the border and replaced it with catch-and-remove. We ended the practice in which non-Mexican aliens who were first apprehended were then let go after receiving a notice to appear in court. They are now being detained for as long as it takes to send them back to their home countries.

Recently, we awarded the contract for SBInet, the high-tech component of our border security efforts. It includes the building of a virtual fence with a full array of ground-based radar, cameras, and unmanned aerial systems. Through Project 28 in Arizona, we are in the process of deploying and validating the first 28 miles of what will be another key element in our border security strategy.

Building the virtual fence should fuel the progress we've been witnessing at the border, chiefly the decline in illegal border crossings, since launching our other initiatives. Over the past fiscal year, overall apprehensions by our Border Patrol have fallen by 20%. Northern border apprehensions have declined by 7%, while southwestern border apprehensions have dropped by 21%. Moreover, Border Patrol OTM apprehensions are down 39%. Yuma Sector apprehensions have plunged by 68%, Del Rio Sector apprehensions by 48%, and El Paso Sector apprehensions by 40%.

A recently released Pew research report concurred that apprehensions have been declining since the second quarter of last year. The study also indicated that foreign-born Hispanic employment showed the smallest increase since mid-2003. And it revealed that after rising steadily for several years, the growth in remittances to Mexico slackened markedly in mid-2006 and the rate of remittance growth diminished through the first quarter of this year. Taken together, these measures strongly suggest that cross-border migration from Mexico continues to decline significantly.

Interior Enforcement

As mentioned, our battle to protect America from dangerous individuals begins overseas. It does not, however, end at our land borders. It is the job of our ICE agents and officers to ensure that those who have succeeded in crossing our border illegally, including those who pose a threat to our security, are apprehended and removed to their home countries. In fiscal year 2006, ICE removed a record 198,511 illegal aliens from the country.

Over the past year, we have stepped up our efforts to hold employers accountable for illegally hiring some of these individuals. Indeed, ICE has made 3,942 administrative arrests and 790 criminal arrests in worksite enforcement cases this year alone.

E-Verify

Most employers do not want to hire illegal workers. To help them avoid doing this inadvertently, we have a voluntary program, called E-Verify, that lets them check the work status of their new hires online. This system compares information from the I-9 Employment Verification form, which establishes work eligibility, against the Social Security Administration and DHS immigration databases. The system is quick, easy, and free and more than 21,000 employers rely on it.

Last month, we announced our intent to expand this successful system. Beginning on October 1, 2007, all federal departments and agencies must begin verifying new hires through E-Verify. We also are encouraging contractors in enroll in E-Verify. In addition, we plan to modify our Homeland Security Acquisition Manual to include a vendor's participation in E-Verify as a consideration during the DHS procurement evaluation process. Finally in order to prevent document fraud and identity theft, E-Verify will include a photo screening tool. This tool will work by allowing an employer to check the photo on the Employment Authorization Document or Permanent Resident Card presented by their new hire against the photo DHS has for that document from the 14.8 million photo images stored in DHS immigration databases.

SSN/No Match

As part of our announcement about expanding and enhancing E-Verify, we also issued a final regulation that outlines specific steps employers should take upon receiving a "no-match" letter from the Social Security Administration informing them of an employee whose name and Social Security Number do not match government records. There can be many causes for a no-match, including clerical errors and name changes. One potential cause might be a submission of information for an alien who isn't authorized to work in the U.S. and who may be using a false Social Security number or a Social Security number assigned to someone else.

This regulation is currently in litigation and we are defending it vigorously.

Legal Immigration

Thus far, we've focused on how we're enforcing our immigration laws so we can secure our borders and protect our country. Through our U.S. Citizenship and Immigration Services (USCIS), we are also committed to creating a more efficient, effective process for those who are seeking to come here legally.

By the end of September of last year, USCIS reached a tremendous milestone. Its caseload backlog dropped to less than 10,000 from a high of 3.8 million cases in January 2004. In addition, over the past year, it developed and implemented a new fee schedule which will give it the necessary resources to process more than 7 million immigration cases annually.

Thoughts on Immigration Reform

No summary of our progress in protecting America from harmful individuals would be complete without some brief comments on the comprehensive immigration reform bill that stalled in the U.S. Senate.

The failure of the Senate bill to become law meant the defeat of a number of vital, constructive provisions. I want to focus on two of them that could have strengthened our efforts to protect our country from its enemies.

The first of these was the Temporary Guest Worker Program (TWP), which would have established a steady, legal, temporary channel of workers whose skills were in demand by our economy. The second provision sought to deal with the 12 million people who were already here illegally. Those who arrived prior to January 1 of this year and were willing to step out of the shadows, obey the law, and pay a penalty, would have been granted a work visa, renewable after four years, and an opportunity to return to their home country four years later after the first removal and apply for a green card.

Both provisions would have freed our immigration enforcement officers to focus more of their time and effort on apprehending violent criminals, drug traffickers, gang members, and potential terrorists who pose an immediate threat to this country and its people. Without the kind of immigration reform that includes these provisions, our hardworking CBP and ICE officers will instead be compelled to continue their pursuit of hardworking immigrants whose sole crime was coming here illegally.

2. Protecting Against Dangerous Things

As we guard our homeland against threats from individuals, we are simultaneously working to protect it from dangerous cargo. Here, too, we employ a layered approach to security. Our strategy is to keep out dangerous goods by creating rings of protection around our ports of entry and throughout our maritime supply chain, from point-of-origin abroad to point-of-destination here.

An Expanding Perimeter: Overseas Measures

Our outermost security layer is overseas.

One step we've taken is to create a public-private and international partnership with more than 7,000 businesses, including most of the largest U.S. importers. Through our Custom-Trade Partnership Against Terrorism, or C-TPAT, we are reviewing the security practices not only of companies that ship goods, but also those that provide them with services. Our goal is to inculcate a security-consciousness among firms that are involved at every point in the supply chain.

As of the last fiscal year, C-TPAT participants, combined with Importer Self-Assessment (ISA) participants, accounted for almost half of all import value and 31% of all entries.

With respect to the cargo itself, we employ risk-based targeting, where we use an automated targeting system to screen 100% of U.S.-bound containers prior to their arrival here. This is done by collecting information about every incoming shipment 24 hours prior to the container being loaded at a foreign port. This information includes content, manifest, shipping history, and other data. We have made great progress, in partnership with industry and trade groups, toward obtaining additional data elements that will enhance the targeting systems. Through our Container Security Initiative or CSI, CBP officers, working with port officials, examine this information in order to identify those high-risk containers that require further inspection. These efforts underscore the necessity of a layered, risk-based approach to global supply chain security.

Over the past year, we have expanded our CSI program. By the end of this year, CSI will be active in more than 58 overseas ports, covering 85% of U.S.-bound cargo.

In our efforts to detect dangerous cargo overseas, we remain particularly concerned about nuclear terrorism, specifically about a radiological or nuclear device -- or the material needed to make one – entering our country.

Since 9/11, our Department, the Department of Energy, Department of State, and other interagency partners have taken significant steps in conjunction with the private sector and our overseas allies to counter this lethal threat to maritime commerce.

We have done so with the vital cooperation of Members of Congress, who earlier last year passed the SAFE Port Act to further institutionalize these efforts.

In order to build on these efforts, last December, we launched our Secure Freight Initiative. Under this initiative, the U.S. government is placing radiation detection equipment, imaging machines, and optical character readers at terminals in an initial set of seven foreign ports. Three of these ports will scan 100% of the cargo coming to this country, fulfilling the requirements of the SAFE Port Act. Operation testing on a more limited basis will take place at the four remaining locations, providing us information on

how we can address the security challenges associated with larger and more complex ports.

The goal of the Secure Freight Initiative is to allow us to identify radiological or nuclear threats well in advance of a container's arrival to our country. It will provide host governments with greater visibility into potentially dangerous shipments moving across their territory. It will help carriers, shippers, and terminal operators have greater confidence in the security of cargo they move and unload. And by applying our risk management and reduction strategy, it will help resolve threats in a way that keeps safe cargo moving.

Protecting Against Dangerous Cargo At Home

Our layered approach against the threat of nuclear terrorism starts with such overseas measures as the Secure Freight Initiative and continues at our U.S. ports, where we've been significantly expanding our radiation detection capabilities.

Earlier this year, we reached a milestone in that we now have installed 1,000 Radiation Portal Monitors (RPMs) at major seaports and land ports of entry across the nation.

In just two years, we've more than doubled the percentage of incoming containerized cargo being scanned for radiological and nuclear threats at our land borders (from 40% to 97%) and more than quadrupled that percentage at seaports (from about 20% to 91%). By the end of next year, we will scan nearly 100% of inbound cargo containers for such deadly material.

And to help us reach this goal, we are continuing to test what we expect to be the next generation of scanning technology – Advanced Spectroscopic Portals, or ASP. The ASP program is designed to automatically distinguish between naturally occurring radioactive material and dangerous nuclear material that actually poses a threat.

These advanced systems are not only meant to provide enhanced detection capabilities, but also to improve the efficiency of the scanning process. Currently, when a container activates an alarm, our CBP officers must examine the container and the enclosed material to determine whether it poses a threat or is a legitimate import with naturally occurring radiation. It is our hope that ASP technology will reduce false alarms and increase the flow of commerce through our ports, while enhancing security.

ASP systems remain promising. Our next step will be to complete additional field testing and other rigorous certification measures in busy environments. Once we are done, we will report back to Congress with our results before doing a full-scale procurement.

3. Protecting Critical Infrastructure

Dangerous individuals and goods pose a continued threat to our homeland in fundamental ways. One way is by putting our nation's critical infrastructure at risk.

Passenger Planes

The September 11th attacks underscored how much damage dangerous individuals can inflict by getting control of passenger planes.

Since 9/11, we have taken substantial steps to improve aviation security, while maintaining the efficiency of air transportation for the traveling public. Highly trained Transportation Security Officers screen passengers and baggage at airports across the country. Federal Air Marshals protect hundreds of domestic and international flights every day. We have hardened cockpit doors, armed pilots to defend the flight deck, and strengthened air cargo security.

Nonetheless, the disruption in August 2006 of the London plot to blow up U.S.-bound transatlantic planes serves as a stark reminder that the threat to air travel remains. Due to this crisis and other events occurring in the United Kingdom, our Transportation Security Administration (TSA) increased Federal Air Marshal deployment to the U.K. as well as other foreign destinations. TSA has also deployed Visible Intermodal Protection and Response (VIPR) Teams to increase security at passenger rail and mass transit locations.

Responding to that threat and to a 9/11 Commission recommendation, last month I announced our Secure Flight rule that would transfer responsibility for watch list checks from the airlines to TSA.

Under this rule, if implemented as proposed, TSA will receive limited passenger information from airlines as early as 72 hours before a flight, check it against the watch list provided by the Terrorist Screening Center, and transmit the results back to aircraft operators. In the case of a watch list match, TSA will have time to coordinate the appropriate action, including, if necessary, preventing a person from boarding the plane.

Essentially, this takes an already-existing security measure – comparing passenger information against the terrorist watch list – and streamlines the process by giving this responsibility to TSA rather than dozens of different air carriers. This will ultimately enhance security, create a more consistent and uniform pre-screening process, and reduce potential misidentification issues for passengers.

What this will not do is harm privacy, use commercial data, assign a risk score to passengers, or predict behavior.

TSA will only collect the minimum amount of personal information necessary to conduct effective watch list matching and prevent misidentification.

We have also issued a Privacy Impact Assessment and Privacy Act System of Records Notice that outlines how TSA collects, uses, stores, protects, and retains personally identifiable information as part of the Secure Flight Program.

In addition, our Traveler Redress Inquiry Program – or DHS TRIP – is available for passengers who feel they have been improperly delayed or prohibited from boarding an aircraft.

We will test this system and work with the travel industry, airlines and other stakeholders in the development of the Secure Flight program and will take public feedback during the comment period.

Our concern about passenger planes is not limited to the problem of dangerous people boarding them. We are also focused on the risk of dangerous cargo entering them. Last year, we issued a new air cargo regulation that mandates 100% inspection of passenger parcels that are presented at airport counters. We also put in place stricter inspection requirements for air cargo shippers and indirect carriers.

In the next fiscal year, we plan to invest $56 million to fund 300 air cargo inspectors, K9 teams and technology which will allow us to track carriers, shippers, and support risk-based air cargo screening across the entire supply chain.

Sector-Specific Plans/NIPP

Passenger planes are an integral part of our transportation system, which under Homeland Security Presidential Directive 7 is one of the 17 sectors that comprise our critical infrastructure.

Each of these 17 sectors is different, with its own unique needs, risks, and interdependencies.

The private sector, not the federal government, owns and operates most of this infrastructure. Government and the private sector must work together to set goals and priorities, identify key assets, assign roles and responsibilities, target resources, and measure our progress against national priorities.

In June of last year, we released the National Infrastructure Protection Plan (NIPP) to provide an overarching framework. The NIPP is our unifying structure for understanding and managing risk to the nation's infrastructure – created in partnership with the private sector.

A critical part of the NIPP includes the Sector Specific Plans, which drill down to the sector level and provide the nuts and bolts of how each of the 17 critical sectors identifies key assets, develops and implements protective programs, and measures progress.

In May of this year, we saw the completion of all 17 Sector Specific Plans of the NIPP. It represents the first time in our nation's history that the government and the private sector have come together on such a large scale – literally, across every major sector of our economy – to develop a joint plan to protect key assets and resources.

The goals of the Sector Specific Plans are to define roles and responsibilities within each sector, catalog existing security authorities, institutionalize security partnerships already in place; and set clear goals and objectives to reduce risk.

The completion of the Sector Specific Plans is a tremendous milestone for our Department, the private sector, and the American people.

Of course, a plan is only as good as its implementation. We look forward to continuing our work with our private sector partners as we work under these plans to manage the risk to critical infrastructure.

Chemical Security

Let me focus on our progress in protecting one of our 17 sectors, the chemical sector.

One of the things we are most concerned about are industrial chemicals being used as weapons – whether through an attack against a chemical facility or an attack against chemicals in transit.

We must tackle this challenge comprehensively. That means securing not only chemical sites and facilities, but chemicals in transit. It means securing the end points of the system as well as the links in between.

The vast majority of chemical shipments do not pose a threat to people. In fact, less than one percent of all shipments traveling by rail are Toxic by Inhalation (TIH), which means if attacked, they could create an airborne hazard and endanger a lot of people.

For this reason, last December we put forward a proposed regulation to reduce the standstill time for rail cars carrying TIH hazards around our major cities. This regulation formalizes a set of agreements we've reached with rail carriers to make sure that the relatively small number of cars that carry TIH chemicals on a given day are not left unattended, can be efficiently tracked, and take the safest, most economically practicable route.

This is risk management in action: targeting the highest-risk chemicals and working with industry to demonstrably reduce that risk without breaking the system.

In April of this year, we published an interim final chemical facility security rule. We are now enforcing that regulation, which, for the first time, sets national risk-based standards for chemical security.

Facilities that fail to meet our performance standards could face penalties of up to $25,000 for each day a violation occurs, or they could be ordered to halt operations until security is brought up to a level that meets certain performance standards.

I am confident that most chemical plants will accomplish what we need to get done in the area of security. That is because this industry understands that investments in security help protect its operations.

Ultimately, chemical security is not solely a federal responsibility; it is a shared responsibility, not just among federal, state and local governments, but also with the private sector.

Field Applications: HITRAC, JFK Plot Detection/Disruption, Hurricane Scenarios Analysis

No discussion of critical infrastructure protection would be complete without talking about how we are applying our capabilities to actual threats.

One way is through the Homeland Infrastructure Threat and Risk Analysis Center (HITRAC), a shared program between our National Protection and Programs Directorate (NPPD) and our Office of Intelligence and Analysis (I&A). Through HITRAC, we are improving information sharing by developing three new product lines tailored to meet the intelligence needs of the private sector and state and local governments, including sector-specific documents, unclassified communication with the private sector and quarterly suspicious activity reporting analyses.

Last June, through information sharing and close coordination between DHS and the FBI, as well as with pipeline owners, the U.S. government was able to announce the thwarting of an alleged plot to attack the fuel tanks and pipelines at New York's JFK Airport. During the investigation, we were able to identify vulnerabilities that might be targeted by the plot.

Another application of our strengthened critical infrastructure capability concerns threats posed by natural disasters. We now have an enhanced capacity to map out the various scenarios of a predicted hurricane making landfall in a particular area. We have strengthened our ability to predict the probable effect on existing infrastructure of hurricanes of various categories, enabling us to tailor our disaster responses accordingly.

We are also continuing to strengthen the security of our cyber infrastructure.

4. Building an Effective Emergency Preparedness and Response System

As we work to protect our critical infrastructure by preventing disasters from occurring, we must also ensure that our nation is well-prepared to respond to disasters – natural as

well as man-made – when they do occur. We are reminded of this as we reflect on the recent second anniversary of Hurricane Katrina.

Improving Interoperable Communication Among First Responders

When it comes to disaster preparedness and response, one of our most important priorities at DHS is interoperable communications. This refers to the ability of first responder agencies – whether fire, police, or emergency medical services – to communicate during an emergency or disaster. Interoperability means having radios and other devices that can talk to each other, protocols and procedures for communication, and clear lines of authority.

Improving interoperable communications is a subject that the 9/11 Commission discussed in its final report and said must be a priority for all levels of government.

Much progress has been made since 9/11 to achieve tactical, command-level interoperability in our major high-threat urban areas. Over the past two years, DHS has assisted 75 urban or metropolitan areas in developing and exercising tactical interoperable communications plans. Our Interoperable Communications Technical Assistance Program has been instrumental throughout this process.

Through our Public Safety Interoperable Communications (PSIC) grant program, which we will co-administer with the Department of Commerce, we will provide an additional $1 billion in interoperability grants by the end of 2007. By the end of this year, DHS will have provided over $4 billion to state and local governments to develop interoperable communications. We are requiring that each state and territory submit a communications plan by December 1 to ensure eligibility for the PSIC grants.

And in April of this year, our new Office of Emergency Communications began operations in accordance with the Homeland Security Act of 2002. Its job is to improve interoperable communications for our public safety partners and across federal, state, and local governments.

A good example of a region with effective interoperable communications is right here in the National Capital Region. Today, all first responders in this region – whether in Maryland, DC, or Virginia – are able to communicate with each other. Fire fighters and police not only can talk to each other within the same jurisdiction, they can communicate across jurisdictions.

So how is the rest of the country faring on interoperability?

Last December, we released the findings of our national baseline survey, the first-ever nationwide assessment of interoperability across our country.

We found that roughly two-thirds of emergency response agencies across the nation use interoperable communications at varying degrees. Specifically, response agencies tend to be more developed in their use of technology; interoperability at local levels tends to be more advanced than it is between state and local agencies; and law enforcement, fire response and EMS agencies reported similar levels of development in most areas of interoperability.

In January of this year, we issued interoperability scorecards to 75 urban and metropolitan areas that looked at three things: governance, standard operating procedures, and equipment.

Overall, the scorecard findings show that urban and metropolitan areas have made progress in improving their interoperable communications capabilities. The findings also identify gaps and areas for continued advancement. Key findings include:

- Policies for interoperable communications are now in place in all 75 urban and metropolitan areas.

- Regular testing and exercises are needed to effectively link disparate systems to allow communications between multi-jurisdictional responders (including state and federal).

- Cooperation among first responders in the field is strong, but formalized governance (leadership and strategic planning) across regions needs further improvement.

One particular urban area that scored well in our survey was Minneapolis/St. Paul. That area's capability and training were put to good use in delivering a prompt response to the recent collapse of the I-35 bridge.

We are confident that by the end of 2008, all 75 of our country's largest urban areas, 50 states, and 6 U.S. territories will have demonstrated a minimum level of emergency response interoperable communications, thus fulfilling a major post-9/11 national goal.

FEMA: Reorganization, New Leadership, Enhanced Capabilities

Besides improving interoperable communications among our nation's first responders, we are also committed to continued progress in the way our own Department deals with emergency preparedness and response through FEMA.

While Congress mandated changes to FEMA's organizational structure, we have made modifications to create a more nimble, better equipped organization. FEMA now includes the U.S. Fire Administration, the former Office of Grants and Training, the

Chemical Stockpile Emergency Preparedness Program, the Radiological Emergency Preparedness Program, and the Office of National Capital Region Coordination.

We have created an Office of Health Affairs outside of FEMA to coordinate the Department's medical preparedness efforts. This office will work closely with FEMA and all of our component organizations as well as our external partners such as Health and Human Services.

We have created the National Protection and Programs Directorate to unify our infrastructure protection, risk-management, cyber security and communications, and US-VISIT border management functions.

FEMA is no longer stove-piped into Response and Recovery Divisions. It now has new Directorates of National Preparedness and Disaster Operations which will focus on long-term preparedness and response planning. It also has robust Logistics Management, Disaster Assistance, and Disaster Operations Directorates.

We have also strengthened FEMA's 10 regional offices, led by regional administrators who work directly with state and local emergency management communities. All 10 regional directors are now in place.

Ultimately, FEMA's success is tied to the relationships it builds within FEMA regions with emergency managers and state and local communities. In this regard, under the new structure, we now have a National Advisory Council to serve as an avenue for our partners to provide input into the Department's policies and programs, and we will create Regional Advisory Councils to work at a regional level.

Of course, we must continue to implement the National Incident Management System (NIMS) to ensure a common framework for emergency response across our country. We all have to be on the same page when disaster strikes. Over the next two years, we will continue to work to strengthen the NIMS and to work for its full adoption.

USCG Deployable Operations Group (DOG)

In addition to FEMA, the U.S. Coast Guard continues to play a vital role in the building of a 21st century emergency response system. Two years ago, in response to Hurricane Katrina, the Coast Guard helped save over 33,000 lives, a remarkable feat.

Over the past year, we have strengthened the Coast Guard's capabilities by creating a Deployable Operations Group (DOG) consisting of six Coast Guard elements: the National Strike Force, Port Security Units, Maritime Safety and Security Teams, Tactical Law Enforcement Teams, Naval Coastal Warfare Personnel, and Maritime Security Response Teams.

Each of these elements has unique capabilities, including search and rescue, hazmat, biological and chemical response, counterterrorism, law enforcement, and port security

expertise. By bringing them under a single command and training them for rapid deployment in any environment, we are strengthening our ability to respond effectively to any disaster. Moreover, by coordinating this group with other DHS assets, such as FEMA Search and Rescue teams, ICE officers, and CBP agents, we can create an efficient, tailored, DHS-wide response to any incident.

5. Strengthen and Unify DHS Management

If we are to strengthen our ability to protect America from disasters and to respond effectively when they happen, we must continue to improve our own internal operations at DHS.

Integration

When our component agencies entered the department on March 1, 2003, we faced one of the greatest integration challenges of modern times. The Department effectively had 22 separate human resources offices, 8 payroll systems, 19 financial management centers, and 13 procurement systems.

We have made remarkable progress to integrate these functions. We are working to consolidate 17 major data centers into just two. This will give us robust, resilient data management and save millions of taxpayer dollars.

Of course, a Department of our size must have straightforward, transparent, and well-managed contracting and procurement practices and vehicles. Otherwise, we are leaving the door open to fraud, waste and abuse.

We have implemented two programs that will help make sure our IT procurement and contracting houses are in order – FirstSource and EAGLE. FirstSource consolidates our IT portfolio and establishes Department-wide contracts for commodity purchases. EAGLE will allow our agencies and components to meet their IT needs on a competitive and as-needed basis, rather than ad-hoc or through large, wasteful contracts.

To coordinate all of this work and ensure the prudent annual investment of over $3 billion in information technology, it is essential to have a strong Chief Information Officer who is empowered to make decisions, control spending, and ensure consistency.
In March of this year, we issued a management directive elevating the authority of our Department's Chief Information Officer. By doing so, DHS will be at the forefront of fulfilling the promise of the Clinger-Cohen Act of 1996 which established the role of the CIO at major federal agencies.

Each DHS component will be required submit its IT budget to the CIO, who will make recommendations to me for final inclusion in the Department's budget request.

Ensuring Excellence and Diversity in the Workplace

Besides having an integrated Department, we must continue to recruit and maintain a first-class homeland security workforce.

One way of measuring our progress is by looking at vacancy rates in critical areas of our Department. DHS is clearly on track to fill all vacant positions in mission-critical occupations this fiscal year. As of last month, the vacancy rate was 2.92% for frontline occupations in CBP, 8% at ICE, and 4.3% at FEMA.

In July of this year, the Majority Staff of this Committee issued a report claiming that 24% of our Department's top-level executive positions were vacant, but this percentage was artificially inflated due to OPM's recent authorization of 73 new SES positions. Without the 73 new positions, the vacancy rate for top positions would only be 12%. Moreover, even when we include the OPM authorization, the vacancy rate has already fallen to 22% as of last month. In addition, 97 of 125 vacant positions are in the process of being filled.

We believe that a first-class workforce should reflect the diversity of our nation and so several of our component agencies have active minority recruitment programs, including the Coast Guard, Secret Service, Customs and Border Protection, and the Transportation Security Administration, among others. We continue to seek minorities and students from Historically Black Colleges and Universities (HBCUs). We are also entering partnership agreements with the Black Executive Exchange Program (BEEP) of the Urban League, the National Association of Hispanic Federal Executives (NAHFE, and the Hispanic Scholarship Fund Institute. We are pursuing the services of an executive search firm with a proven record in attracting and recruiting people from diverse backgrounds for executive positions.

In addition, our Science and Technology Directorate's University Centers of Excellence program has partnered with three HBCUs to conduct vital homeland security-related research and to educate the next generation of homeland security experts and scholars.

Since our inception, we have made a commitment to provide opportunities for small businesses to participate in our procurement program, including those small businesses owned by minorities, women, disabled veterans, veterans, and those located in economically distressed areas.

Transition Planning

Along with promoting integration and workplace diversity and excellence, we also continue to implement our plans to ensure our Department's transition to the next administration in January 2009.

As we have seen recently in the U.K., terrorists seek to exploit any perceived weakness that may occur during a period of government transition. DHS simply cannot afford to have a "down period" between the end of this administration and the start of the next.

So we are establishing detailed continuity plans, and ensuring protocols and procedures are in place for the next leadership team. But more importantly we're training and cross-training our senior career employees to ensure that each component and office within DHS has capable leadership ready to take the reins as new appointees adjust to their positions.

GOALS FOR THIS YEAR AND THE FUTURE

As we look to the future, we are determined to continue advancing the priorities of our Department in fulfillment of our homeland security mission. Rather than providing an exhaustive list, I'd like to cite a few key examples of how we intend to build on the past year's accomplishments as outlined in this testimony.

1. WHTI Implementation and REAL ID

As I noted, if we wish to secure our homeland, secure documentation is essential. That's why we will continue to move forward on our Western Hemisphere Travel Initiative. As I mentioned, in January of this year, we implemented our air travel rule and this June, we announced the proposed rule for WHTI's land and sea portion.

As early as the summer of 2008, we will start to require WHTI-compliant credentials – a passport, PASS card, a NEXUS card, or other acceptable documents as defined in the final rule. We will provide at least 60 days notice before final implementation.

Since this is a significant change, we are going to be reasonable and flexible in implementing the WHTI provisions. We're taking a phased approach that will allow people to get the necessary documents and adjust to the requirements. And we're also making accommodations for children and groups of minors crossing the border, as well as members of our armed forces, round-trip cruise ship passengers, and first responders.

And as part of WHTI, we are also working with the states to develop an enhanced driver's license. Since they will serve as an alternative to a passport or passport card at land and sea borders, enhanced driver's licenses will only be issued to U.S. citizens. They must also incorporate the technology that DHS specifies in order to aid the legitimate movement of travelers.

Our goal is to make enhanced driver's licenses fulfill the requirements of REAL ID. More then two years ago, Congress had passed the REAL ID Act in response to the 9/11 Commission's recommendation that the federal government "set standards for the issuance of….sources of identification, such as driver's licenses." Secure driver's licenses are essential for secure identification.

Last March, in accordance with the REAL ID Act, I announced a rule that proposed specific minimum standards for state-issued driver's licenses and identification cards to be accepted for federal purposes, such as air travel.

Under these standards, applicants for driver's licenses would need to bring documents to their state DMV office for the purpose of validating five things: their identity, date of birth, legal status in the United States, Social Security number, and address.

The DMV offices would take photos of applicants, scan or copy the documents the applicants are providing, and then go through a common-sense process of verifying the accuracy or legitimacy of the information contained in those documents.

Now as for the licenses themselves, we proposed standards for the states to ensure that the REAL ID licenses being produced would be hard to tamper with, counterfeit or duplicate for fraudulent purposes.

And finally, we wanted to ensure that drivers couldn't hold multiple licenses in multiple jurisdictions, so our rule would require that each state check to make sure that no other state already had licenses issued to them.

Personal privacy will be protected by states issuing REAL ID driver's licenses. Our proposal requires that each state conduct name-based and fingerprint-based criminal history record checks on DMV employees who will be involved in REAL ID in relevant ways.

Through REAL ID, we're not only preserving people's privacy but strengthening it. By improving the quality of our ID documents, we're protecting against one of the fastest growing crimes in America today – the crime of identity theft. There is no greater violation of privacy than when criminals gain total access to personal information in the process of stealing someone's identity. In the same vein, REAL ID should also offset the cost of reissuing new licenses through the savings that people will realize by the reduction of identity theft crimes.

When we announced the REAL ID rules in March, we said that states which seek justifiable extensions and timetables will have through December 31, 2009 to come into compliance.

We believe that delay in implementing REAL ID could be detrimental to our national security. In the National Intelligence Estimate that was released in July, it clearly states that Al Qaeda will "intensify" its efforts to put operatives inside our country. Clearly, time waits for no one and neither do our enemies. Across the nation, the American people support the creation of secure driver's licenses and other forms of identification that cannot be exploited or forged by terrorists. Our states have an obligation to their people to respond to what the 9/11 Commission recommended and what this Congress affirmed. They have a duty to help us repair the security gaps that were so tragically exploited on 9/11 by implementing REAL ID as quickly as possible.

2. Border Security

I also testified about how we are securing our homeland by strengthening our border security. As I mentioned, as part of that commitment, we will have more than 18,000 Border Patrol agents by the end of 2008, double the number we had before 2001. By the end of next year, we also intend to ensure that there are 370 miles of fencing along our southern border, 300 miles of vehicle barriers, three additional UAVs, and 105 camera and radar towers. We will also work to ensure that 1,700 more Border Patrol Agents and an additional UAV are added in 2009.

3. General Aviation and Small Vessels

When I discussed earlier how we are working to protect our infrastructure from dangerous people and cargo, I mentioned passenger planes. We need to address these issues.

Accordingly, this month, we are publishing a Notice of Proposed Rule Making that proposes new passenger screening requirements for private aircraft entering into and departing from the United States. Currently we only receive very basic information from private aircraft entering the U.S. These proposed requirements would bring private aircraft into closer alignment with the passenger screening requirements that currently apply to commercial air carriers under CBP'S APIS regulation and allow inspectors more time to fully pre-screen travelers and crews and take necessary actions to resolve threats, whether that means denying entry into U.S. airspace, re-routing an aircraft, or meeting the aircraft upon arrival.

We are also concerned about four potential security threats with regard to the more than 17 million small boats, ranging from commercial enterprises to passenger ferries to canoes and personal watercraft.

First, we're concerned about their use to smuggle weapons, including a weapon of mass destruction, into our country. Second, we're concerned about their use as a water-borne improvised explosive device, a use which was actually deployed in 2000 through al-Qaeda's attack on the U.S.S. Cole. Third, we want to prevent the use of a small vessel to smuggle dangerous people into our country. And finally, we're concerned about these boats being used as launching pads for an attack on the maritime industry or on critical infrastructure.

Now how do we defend against these threats? The short answer is by applying the same risk-management, partnership, and layering principles I've already outlined.

Through the various initiatives I've already discussed, we are indeed making strides in protecting our ports from these kinds of threats. But we also need to consider measures that are specifically geared to small vessels.

We need such measures to enhance protection and yet balance our need for freedom of movement, privacy, and economic vitality.

4. Fusion Centers

If we're going to progress in our efforts to protect people and critical infrastructure across our nation, we need to concentrate more on how we share accurate, timely, actionable intelligence, particularly with state and local governments. To that end, we are increasing our participation in state and local fusion centers (SLFCs). Our goal is to help build a national fusion center network.

In June of last year, I designated our Office of Intelligence & Analysis (I&A) as the Executive Agent to manage a program that is designed to advance our SLFC mission. Last month, this program was codified the law implementing the 9/11 Commission's recommendations.

We are now working with the Department of Justice and other members of the Information Sharing Council to gather and assess responses provided by every state and major urban-area fusion center to a capacity assessment of fusion centers. To date, DHS has assessed 25 Fusion Centers, 13 of them in the past year. We plan on conducting assessments at 10 more centers in fiscal year 2008.

Based on the results of the assessments and other factors, DHS has deployed 17 intelligence officers to 17 State Fusion Centers as well as to major city or regional centers in New York City, Los Angeles, and Dallas. DHS plans to have officers in as many as 35 sites by the end of fiscal year 2008.

5. Continued Integration

And finally, if we want to meet our goals in the coming years, it is essential that we continue our efforts to build a unified, integrated Department of Homeland Security.

Through our OneNet program, we are consolidating seven legacy Wide Area Networks into a single Departmental network. OneNet will give us a secure, standard platform to facilitate information flow and streamline our IT infrastructure. We expect to complete OneNet integration by October 2008.

Under HSPD-12, we are also creating a single, tamper-proof smartcard for all DHS employees. And we have put in place a plan to transition the Department's headquarters to a single campus over the next ten years.

One of the key benefits of a fully integrated Department is the ability to apply joint doctrine, planning, training and exercising across our agencies.

As mentioned earlier in my testimony, over the past year, our U.S. Coast Guard created from six of its teams a single Deployable Operations Group which combines their search and rescue, hazmat, biological and chemical response and other capabilities and trains

their members for rapid deployment in the event of a disaster. We intend to make this a model throughout our Department as we seek to apply fully the benefits of integration.

And we also intend to keep moving forward on our National Strategy for Maritime Security. Issued in September 2005, it seeks to align federal government maritime security programs into a comprehensive national effort involving federal, state, local, and private sector entities. The eight supporting plans address the specific maritime threats and challenges. For example, the October 2005 Maritime Operational Threat Response (MOTR) plan describes the U.S. government's plan to respond specifically to maritime terrorism threats or incidents, including the roles and protocols of the various agencies, and the need for additional planning.

Clearly, a unified, integrated DHS is essential to the security of this nation. Earlier this year, it was a unified, integrated DHS that worked with our international partners to ensure an appropriate response to the London/Glasgow vehicle-borne IED attacks.

CONCLUSION

Since its inception more than four years ago, our Department has worked hard to fulfill its mission of protecting our homeland. While challenges remain, from terrorism to natural disasters, we have made our country safer and our people more secure.

From the beginning, we have understood that we cannot fulfill our mission alone. That is why we continue to value our partnerships, including our relationship with Congress. Indeed, Congress has been invaluable in helping us advance our goals and will remain a key partner in the months and years to come.

Members of Congress have played a vital role in many areas. We appreciate their efforts to help us reorganize FEMA. Now it is time to let a reorganized FEMA do its job.

We are grateful for their passage of REAL ID. Now it is time to consider passage of other critical 9/11 Commission recommendations, including Congressional oversight reform, as well as legislation authorizing us to regulate potentially hazardous chemicals such as chlorine.

I want to thank this Committee and Members of Congress again for their support and I look forward to our working together in the future to fulfill our mandate on behalf of this nation and its people.